Exploring the Impacts of Intrinsic Variables on Security Compliance Efficiency Using DEA and MARS

Charlette Donalds, Kweku-Muata Osei-Bryson, Sergey Samoilenko

Exploring the Impacts of Intrinsic Variables on Security Compliance Efficiency using DEA & MARS

Charlette Donalds[1[0000-0002-9209-0984 ✉]], Kweku-Muata Osei-Bryson[2] and Sergey Samoilenko[3]

[1] University of the West Indies, Mona, Kingston, Jamaica
charlette.donalds02@uwimona.edu.jm
[2] Virginia Commonwealth University, USA
KMOsei@VCU.edu
[3] Averett University, USA
ssamoilenko@Averett.edu

Abstract. Given that appropriate human behavior is required to minimize the occurrence of cybersecurity breaches, the issue of *security compliance* is critical. Within this context organizations would be interested in the efficient achievement of *security compliance*. In this paper we explore the concept of *Security Compliance Efficiency*, and present a hybrid DEA+MARS methodology for identifying its antecedents. We also present resulting examples of relationships that describe the impacts of intrinsic variables on *Security Compliance Efficiency*.

Keywords: Security Compliance Efficiency, Data Envelopment Analysis (DEA), Multivariate Adaptive Regression Splines (MARS).

1 Introduction

The current era is dominated by the use of information and communication technologies (ICTs) in the lives and activities of individuals, organizations and governments. However, increased adoption of ICTs is positively correlated with increased economic loss and technological threats and/or attacks. For instance, the average cost of cybercrimes to organizations increased by 23 percent in 2017 over 2016, reaching US$11.7 million [1]. Too, the WannaCry ransomware attack in May 2017 affected more than 300,000 victims in 150 countries [2]. To cope with these technological or cybersecurity threats, security stakeholders have implemented technology-based protection solutions and conducted cybersecurity awareness activities for users. Users are recognized as key threats to achieving security because they often fail to adhere to the security best practices. According to researchers, users are often considered the “weakest link in the chain” of system security but are also considered the greatest assets to reduce potential security threats [3-5].

To influence users’ *security compliance* behavior, the literature offers some antecedents. In general, studies report that increased security awareness initiatives positively influence users’ compliance behavior [6-10] and specially, Bulgurcu, Cavusoglu and Benbasat [6] and Donalds [8] found support for the direct link between general security awareness (*GSAW*) and users' *security compliance* behaviour (*SECC*).

Self-efficacy (*SLEF*) is another factor cited to influence users' behavior generally. According to protection motivation theory, *SLEF* emphasizes an individual's ability or judgment of his or her ability to perform an action [11]. More specifically, the theory suggests that increasing individual's *SLEF* can improve their competence in coping with a task. In a computer training course *SLEF* was found to be a strong influence on individuals' performance in their use of the computers [12]. Additionally, Donalds and Osei-Bryson [13] offer empirical support for the influence of security self-efficacy on *SECC*.

While the constructs referenced above can be considered to be extrinsic to the individual and thus subject to be influenced by organizational efforts, others are more intrinsic. One such construct is general security orientation (*GSOR*). *GSOR* is intrinsic since according to Ng, Kankanhalli and Xu [14], an individual with a greater predisposition towards computer security should exhibit higher levels of *security compliance* behavior. *GSOR* has also been shown to be significantly correlated with *SECC* [13].

Another intrinsic construct, *Gender*, has also been shown to have a profound influence on an individual's perceptions, attitudes and performance [15]. Results from studies in the domain have also found gender to be significantly correlated with employees' *security compliance* intention and behaviour [9, 16-18].

More recent results from Donalds and Osei-Bryson [13] suggest an individual's dominant decision style (i.e. *Analytical*, *Behavioral*, *Conceptual*, *Directive*) and dominant orientation (i.e. *Idea* vs. *Action*), which are intrinsic to the individual, also impact *SECC*. Rowe & Boulgarides [19] note that cognitive theorists have long argued that an individual decision style is an important determinant of behavior. Too, others report that an individual's decisions seem to be a function of the individual's cognitive makeup [e.g. 20, 21].

Various studies, including Donalds and Osei-Bryson [13], have attempted to identify the antecedents of *security compliance* behavior. In general, prior studies have concentrated on the issues of efficacy and effectiveness of the relationships between the antecedents of and *security compliance* behavior, however, in this study we take it a step further. In this study we focus on the efficiency of the relationships between the antecedents of and *security compliance* behavior. In other words, previous studies have placed emphasis on "doing the right thing", while the current study inquiries into whether "doing the right thing is done the right way". This focus is of particular importance in the context of the settings characterized by limited resources.

Overall, prior security studies can be considered to be aimed at identifying the relationship described generically as:

$$Compliance = f(Intrinsic\ Inputs, Discretionary\ Inputs) \qquad (1)$$

where *GSAW* and *SLEF* are the *Discretionary Inputs*, and *Gender*, *GSOR*, *Dominant Individual Decision Styles* (DominantDS) and *Dominant Orientation* are the *Intrinsic Inputs*.

In this paper we explore the concept of *Security Compliance Efficiency* and its relationships with intrinsic antecedents, where *Security Compliance Efficiency* is defined as:

$$\textit{Security Compliance Efficiency} = f_{Output}(\textit{Compliance})/f_{Input}(\textit{Discretionary Inputs}) \quad (2)$$

such that its values fall in the [0, 1] interval with the top value indicating the highest level of relative efficiency. For illustrative purposes, using the Donalds and Osei-Bryson [13] causal model, presented in Figure 1, we investigate the concept of *Security Compliance Efficiency*. We adopted this model as it identifies both intrinsic and discretionary inputs, elements salient to our work.

In the context of the causal model of Donalds and Osei-Bryson [13] we would have:

$$\textit{Security Compliance Efficiency} = f_{Output}(\textit{SECC, PWDC})/f_{Input}(\textit{GSAW, SLEF}) \quad (3)$$

thus, a relatively efficient individual is one who has the same level of *compliance* as another individual though his/her *GSAW* and *SLEF* levels are lower, or has a higher level of *compliance* as another individual though their *GSAW* and *SLEF* levels are the same.

Organizations would be interested in knowing the impacts of non-discretionary variables (e.g. *Gender*, *GSOR*, *Dominant Individual Decision Styles* & *Dominant Orientation*) on *Security Compliance Efficiency* since this would help them to identify the situations in which they can invest less while achieving the same level of *compliance*. Further, this would be of particular importance to organizations with budget and other types of resource constraints, including small and medium enterprises (SMEs) and other types of enterprises in developing countries. For it is known that SMEs are essential to the poorest countries in the world where they serve as an important driver of economic growth that accounts for majority of all businesses [22]. Moreover, African SMEs are also important to the global economy because their presences and success create "…a growing middle class with disposable income, in tandem with market opportunities for new investors" [23].

2 Overview of supporting analytic methods

In this study we use a two-stage Data Envelopment Analysis (DEA) based approach [e.g., 24] that involves utilizing the DEA methodology to generate the *Security Compliance Efficiency* scores, then use the Multivariate Adaptive Splines (MARS) statistical analysis method to explore the relationships between the intrinsic non-discretionary inputs (i.e. *Gender*, *GSOR*, *Dominant DominantDS*, and *Dominant Orientation*) and *Security Compliance Efficiency*.

2.1 Overview of data envelopment analysis

DEA is a nonparametric method of measuring the efficiency of decision-making units [25]. Any collection of similar entities could comprise a set of decision-making units (DMUs) and can be subjected to DEA, as long as the chosen entities transform the same type of inputs into the same type of outputs. It has been previously applied to address a wide range of multi-objective and other types of decision making problems [26, 27].

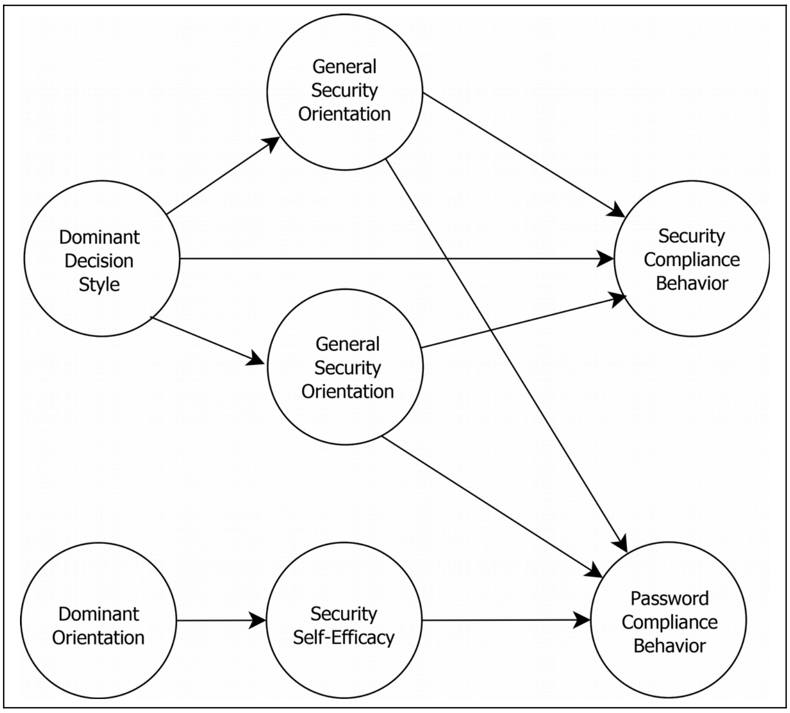
General Security Orientation
Dominant Decision Style
Security Compliance Behavior
General Security Orientation
Dominant Orientation
Security Self-Efficacy
Password Compliance Behavior

Fig. 1. Donalds and Osei-Bryson [13] causal model of security compliance.

The empirical foundation of DEA eliminates the need for some of the assumptions and limitations of traditional efficiency measurement approaches. As a result, DEA could be used in cases where the relationships between the multiple Inputs and multiple Outputs are complex or unknown. Consequently, a DEA model is better perceived as a collection of the Inputs that in some way or form are important to the Outputs of the transformation process under an investigation of a decision maker.

The original DEA model was introduced in 1978 by Charnes, Cooper and Rhodes and it is commonly called the CCR Model. This model allowed representing multiple inputs and outputs of each DMU as a single abstract “meta input” and a single “meta output.” Consequently, the efficiency of each DMU could be represented as a ratio of the abstract input to the abstract output, and the resulting efficiency value could then be used for comparison with other DMUs in the set. By using the techniques of Linear Programming (LP), this comparison results in efficiency ranking of each DMU in the given set, where the highest ranking DMU is considered to be 100% *relatively efficient* and is assigned a perfect score of “1”. Because multiple DMUs could receive the same score, there could be multiple efficient DMUs in the given set. As a result, DEA envelops the data set with the boundary points represented by the *relatively efficient* DMUs – by connecting the boundary points an investigator could obtain a visual representation of the efficient frontier for a given set of DMUs.

The two most common orientations of DEA model are the Input-oriented and the Output-oriented. An *Input-Oriented Model* is concerned with the minimization of the use of inputs for achieving a given level of outputs when inputs are controllable. In the case of an Input-Oriented Model, no DMU would be considered efficient if it is possible to decrease any of its inputs without affecting any other inputs and without decreasing level of the outputs. An *Output-Oriented DEA model*, on the other hand, would be concerned with the maximization of the level of the outputs per given level of the inputs. Thus, it deals with the efficiency of the output production where outputs are controllable.

DEA also allows for accommodating different assumptions regarding *return to scale.* The original CCR model is the most suitable in the case when an investigator has a reason to believe that all DMUs function under the condition of *constant return to scale* (e.g., when the output/input ratio is linear). BCC model [28], on the other hand, is more flexible and allows for considering *variable returns to scale* (e.g., when the output/input ratio is non-linear). Consequently, a DMU that is relatively efficient based on CCR model must also be relatively efficient based on BCC model, but not the vice versa.

2.2 Overview of multivariate adaptive regression splines

Multivariate Adaptive Regression Splines (MARS) is a technique that may be used to discover, describe and evaluate causal links between factors. It has been previously applied to address a wide range of problems [e.g., 29, 30]. While ordinary regression equations attempt to model the relationship between outcome and predictor variables using a single function, the regression splines approach models the relationship between outcome and predictor variables as a piecewise polynomial function $f(x)$ which can be obtained by dividing the range of each predictor variable into one or more intervals and representing f by a separate polynomial in each interval [31]. A regression spline function can be expressed as a linear combination of piecewise polynomial *basis functions* (BF) that are joined together smoothly at the knots, where a *knot* specifies the end of one region of data and the beginning of another. When using MARS for modeling the relationship between the predictor and dependent variables, it is not necessary to know the functional forms of the relationships, as MARS establishes them based on the data. MARS provides the analysis of variance (ANOVA) decomposition, which identifies the relative contributions of each of the predictor variables and the interactions between variables, and handles missing values.

MARS uses both simple and complex BFs. Simple BFs involve a single variable and come in pairs of the form $(x - t)_+$ and $(t - x)_+$ where t is the knot, $(x - t)_+ = \underline{(x - t)}$ if $x > t$, and 0 otherwise; and $(t - x)_+ = \underline{(t - x)}$ if $x < t$, and $\underline{0}$ otherwise [32]. Complex BFs have the form: $h_k(\mathbf{x}) = \Pi_{ij} f_{ij} (x_{i)}$ where $x_1, \ldots x_q$ are the independent variables, f_{ij} is a spline BF for the i^{th} independent variable x_i at j^{th} knot. The function generated using the MARS approach can be described as follows:

$$Y = \beta_0 + \sum_{k=1}^{K} \beta_k h_k (\mathbf{x}) \qquad (4)$$

where β_0 is the coefficient of the constant BF, β_k (k = 1, K) are the coefficients of the BFs, K is the number of basis functions (**BF**) in the model. The coefficient of each BF (i.e. β_k) is estimated by minimizing the sum of square errors, which is similar to the estimation process of linear regression, but involving local data for the given region. MARS provides the analysis of variance (ANOVA) decomposition, which identifies the relative contributions of each of the predictor variables and the interactions between variables, and handles missing values.

Generation of a MARS model involves 2 phases. In the *Forward Phase* BFs are added, allowing the model to become more flexible but also more complex, and terminating when a user specified maximum number of BFs is reached; in the *Backward Phase* BFs are deleted in order of least contribution to the model until an “Optimal” model is found, with the selection of the “Optimal” model being based on the Generalized Cross Validation (GCV) measure. The GCV measure plays a trade-off role between accuracy and simplicity in the generation of MARS models as that played by the Akaike Information Criterion (AIC), Bayes Information Criterion (BIC), and Shwartz Bayes Criterion (SBC) measures play in traditional regression.

3 Research methodology

Our methodology is based on the two-stage DEA model framework but also includes steps to generate appropriate data for this framework, which are as follows:

Step 1: Select an appropriate causal model, and conduct preliminary identification of the discretionary variables and the intrinsic non-discretionary variables.

Step 2: Develop an appropriate data collection instrument.

Step 3: Do appropriate data collection, data understanding, and data cleaning.

Step 4: Do factor analysis and calculation of factor scores.

Step 5: Using the discretionary variables as the inputs and the dependent variables as the outputs, conduct DEA to generate the *Security Compliance Efficiency* scores.

Step 6: Do MARS-based statistical analysis to identify the characteristics of the relationships between the intrinsic non-discretionary variables and *Security Compliance Efficiency*.

4 Application of the research methodology

Step 1 – Select causal model:

We selected Donalds and Osei-Bryson [13] causal model.

Step 2 – Develop appropriate data collection instrument:
Our data collection instrument consisted of two parts: the Decision Styles items as well as the items that measured the antecedents of and *security compliance*. We adopted the standard Decision Styles Inventory (DSI) measures as proposed by Rowe and Mason [33]. We also adopted the items that measured the antecedents of and *security compliance* as proposed by Donalds and Osei-Bryson [13].

Step 3 – Do appropriate data collection, data understanding, and data cleaning:
Our data collect was collected via a web-based survey which was pretested by some IS security experts, faculty members and graduate students. The final instrument was used to collect data from Jamaican employees across multiple industries and faculty members, undergraduate and graduate students from an institution of higher learning. The survey link was sent to faculty members and some Jamaican employees using direct referrals and was advertised in some undergraduate as well as graduate classes. Further, the researchers requested that participants forward the link to other potential participants. As a result, a precise sample frame is difficult to establish. Albeit, the survey was sent/advertised to approximately 510 individuals. We received 248 responses, yielding a response rate of 48.6%. Respondents were from varying industries including education, banking and financial services and telecommunication/IT services. 32.26% of the respondents were males while 67.47% were females.

Step 4 – Do factor analysis and calculation of factor scores:
From the exploratory factor analysis of the *security compliance* items, five factors (i.e., *password compliance behavior (PWDC)*, *security compliance behavior*, *general security awareness*, *general security orientation* and *security self-efficacy*) emerged to explain the maximum portion of the variance in the original variables. These are consistent with the factors identified in the Donalds and Osei-Bryson [13] model.

Step 5 – Do DEA:
We generated 2 DEA models both with an input-orientation with the different scales (i.e. Constant Returns to Scale (CRS) and Variable Returns to Scale (VRS)). The factors that can be considered to be discretionary variables (i.e. *GSAW*, *SLEF*) were used as the input variables for the DEA models. Two factors (i.e. *SECC*, *PWDC*) are associated with *security compliance*, thus we used these factors as the output variables for the DEA models.

Step 6 – MARS-based statistical analysis:

6.1 CRS model: results and discussion
In this model *Security Orientation* (*GSOR*), *Gender*, and *DominantOrientatio*n (i.e. '*Idea*' vs '*Action*") all impact *Security Compliance Efficiency*, often in complex ways (see Table 2.1b). An examination of the 2nd and 4th rows of Table 2.1c suggests that when *GSOR* > 3.00 then *Action-oriented Males* display greater *Security Compliance Efficiency* than *Idea-oriented Males*. Similarly an examination of the 3rd and 4th rows of Table 2.1c suggests that when *GSOR* > 3.00 then *Idea-oriented Females* display

greater *Security Compliance Efficiency* than *Idea-oriented Males*. The reader may recall that given our definition of *Security Compliance Efficiency* then the implication of being less efficient is that *GSAW* and *SLEF* scores would need to be higher to achieve the same level of *security compliance* as the more efficient individual. Thus for such less efficient individuals the organization would need to invest more resources to improve the values of *GSAW* and *SLEF*.

Table 2.1a: Regression equation for CRS.

RHS of Regression Equation
0.774893 + 0.04090968*Max(0, _GSOR_ – 1.33)*(1 if _DominantOrientation_ is “Action”) - 0.117547*(1 if _DominantOrientation_ is “Action”) *(1 if _Gender_ is “F”) + 0.180019* Max(0, _GSOR_-3.00) - 0.260166* Max(0, _GSOR_-2.33) + 0.046970* Max(0, _GSOR_-2.33) *(1 if _Gender_ is “F”)

Table 2.1b: Detailed breakdown of regression equation for CRS.

Dominant Orientation	**Gender**	**GSOR**	**RHS of Regression Equation**
Action	F	< 1.33	0.774893
		(1.33, 2.33]	0.774893 + 0.04090968*(_GSOR_ – 1.33)
		(2.33, 3.00]	0.774893 + 0.04090968*(_GSOR_ – 1.33) - 0.117547 - 0.260166*(_GSOR_-2.33) + 0.046970*(_GSOR_-2.33)
		> 3.00	0.774893 + 0.04090968*(_GSOR_ – 1.33) - 0.117547 - 0.260166*(_GSOR_-2.33) + 0.046970*(_GSOR_-2.33) + 0.180019*(_GSOR_-3.00)
	M	< 1.33	0.774893
		(1.33, 2.33]	0.774893 + 0.04090968*(_GSOR_ – 1.33)
		(2.33, 3.00]	0.774893 + 0.04090968*(_GSOR_ – 1.33) - 0.260166*(_GSOR_-2.33)
		> 3.00	0.774893 + 0.04090968*(_GSOR_ – 1.33) + 0.180019*(_GSOR_-3.00) - 0.260166*(_GSOR_-2.33)
Idea	F	< 1.33	0.774893
		(1.33, 2.33]	0.774893
		(2.33,	0.774893

		3.00]	- 0.260166*(*GSOR*-2.33) + 0.046970*(*GSOR*-2.33)
		> 3.00	0.774893 + 0.180019*(*GSOR*-3.00) - 0.260166*(*GSOR*-2.33) + 0.046970* (*GSOR*-2.33)
	M	< 1.33	0.774893
		(1.33, 2.33]	0.774893
		(2.33, 3.00]	0.774893 - 0.260166*(*GSOR*-2.33)
		> 3.00	0.774893 + 0.180019*(*GSOR*-3.00) - 0.260166*(*GSOR*-2.33)

Table 2.1c: Regression equation for CRS – comparison of impacts.

Dominant Orientation	**Gender**	**GSOR**	**RHS of Regression Equation**
Action	F	> 3.00	0.774893 + 0.04090968*(*GSOR* – 1.33) - 0.117547 + 0.180019*(*GSOR*-3.00) - 0.260166*(*GSOR*-2.33) + 0.046970*(*GSOR*-2.33)
	M	> 3.00	0.774893 + 0.04090968*(*GSOR* – 1.33) + 0.180019*(*GSOR*-3.00) - 0.260166*(*GSOR*-2.33)
Idea	F	> 3.00	0.774893 + 0.180019*(*GSOR*-3.00) - 0.260166*(*GSOR*-2.33) + 0.046970* (*GSOR*-2.33)
	M	> 3.00	0.774893 + 0.180019*(*GSOR*-3.00) - 0.260166*(*GSOR*-2.33)

6.2 VRS model: results and discussion

In this model only *Security Orientation* (*GSOR*), *Gender*, and *DominantDecisionStyle* (i.e. ‘’A’, ‘B’, ‘C’, ‘D’) impact *Security Compliance Efficiency*, but in complex ways also (see Tables 3.2a, 3.2b). An examination of the 1st and 3rd rows of Table 3.2c suggests that when *GSOR* > 3.00 then individual with *Conceptual* decision style display less *Security Compliance Efficiency* than individuals with the other decision styles (i.e. *Analytical*, *Behavioral* and *Directive*).

Table 3.2a: Regression Equation for VRS.

RHS of Regression Equation
0.92517 - 0.13683*Max(0, *GSOR*-1.33) + 0.11648*Max(0, *GSOR*-3.00)

- 0.096062*(1 if *DominantDS* is “C”) *Max(0, *GSOR* -1.33)

Table 3.2b: Detailed breakdown of regression equation for VRS.

Dominant Decision Style	**GSOR**	**RHS of Regression Equation**
C: Conceptual	< 1.33	0.92517
	(1.33, 3.00]	0.92517 - 0.13683*(*GSOR*-1.33) - 0.096062*(*GSOR* -1.33)
	> 3.00	0.92517 - 0.13683*(*GSOR*-1.33) - 0.096062*(*GSOR* -1.33) + 0.11648*(*GSOR*-3.00)
A: Analytic, or *B: Behavioral, or* *D: Directive*	< 1.33	0.92517
	(1.33, 3.00]	0.92517 - 0.13683*(*GSOR*-1.33)
	> 3.00	0.92517 - 0.13683*(*GSOR*-1.33) + 0.11648*(*GSOR*-3.00)

Table 3.2c: Regression equation for VRS – comparison of impacts.

Dominant Decision Style	**GSOR**	**RHS of Regression Equation**
C: Conceptual	> 3.00	0.92517 - 0.13683*(*GSOR*-1.33) - 0.096062*(*GSOR* -1.33) + 0.11648*(*GSOR*-3.00)
A: Analytic, or *B: Behavioral, or* *D: Directive*	> 3.00	0.92517 - 0.13683*(*GSOR*-1.33) + 0.11648*(*GSOR*-3.00)

5 Conclusion

In this paper we have explored the concept of *Security Compliance Efficiency*, and presented a hybrid DEA+MARS methodology for identifying its antecedents. Our search of the research literature did not provide evidence of previous research where the concept of *Security Compliance Efficiency*, as defined in this paper, was previously addressed. Yet given that cybersecurity challenges are common to both ‘developed’ countries and to ‘developing’ countries that are increasingly becoming ICT-oriented, the issue of *Security Compliance Efficiency* is one that needs to be adequately addressed. This paper addresses that gap in the cybersecurity literature that has so far not addressed the *Security Compliance Efficiency* issue. In doing so we have made use of the well-established DEA methodology for generating relative efficiency scores. Rather than using traditional regression analysis for doing statistical analysis we used MARS as it allows us to not only identify if a given variable has a statistically significant impact but also conditions under which it has different types of impacts. It should also be noted that application of our hybrid two-stage DEA+MARS method involved both an input-oriented constant-returns-to-scale (CRS) DEA model, and an input-oriented variable-returns-to-scale (VRS) DEA model.

For illustrative purposes we used the causal model of Donalds and Osei-Bryson [13], but this methodology may be appropriately applied to any other causal model that has dimensions of *security compliance* as its dependent variable(s).

As noted earlier in the paper, organizations would be interested in knowing the impacts of non-discretionary variables on *Security Compliance Efficiency* since this would help them to identify the situations in which they can invest less while achieving the same level of compliance. We identified various non-trivial relationships (e.g. *Idea-oriented Females* display greater *Security Compliance Efficiency* than *Idea-oriented Males*).

References

1. Accenture: 2017 cost of cyber crime study. pp. 54. Ponemon Institute LLC & Accenture (2017).
2. McAfee Labs: McAfee labs threat report, September 2017 (2017).
3. Sasse, M.A., Flechais, I. (eds.): Usable security: why do we need it? How do we get it? O'Reilly, Sebastopol, US (2005).
4. Warkentin, M., Willison, R.: Behavioral and policy issues in information systems security: the insider threat. European Journal of Information Systems 18(2), 101-105 (2009).
5. Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A., Boss, R.W.: If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. European Journal of Information Systems 18, 151–164 (2009).
6. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34(3), 523-548 (2010).
7. D'Arcy, J., Hovav, A., Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 20(1), 79-98 (2009).
8. Donalds, C.: Cybersecurity policy compliance: an empirical study of Jamaican government agencies. SIG GlobDev Pre-ECIS Workshop, Munster, Germany (2015).
9. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18(2), 106–125 (2009).
10. Stanton, J.M., Stam, K.R., Mastrangelo, P., Jolton, J.: Analysis of end user security behaviors. Computers & Security 24(2), 124-133 (2005).
11. Bandura, A.: Self-Efficacy: toward a unifying theory of behaviour change. Psychological Review 84(2), 191-215 (1977).
12. Compeau, D.R., Higgins, C.A.: Computer self-efficacy: development of a measure and initial test. MIS Quarterly 19(2), 189-211 (1995).

13.Donalds, C., Osei-Bryson, K.-M.: Exploring the impacts of individual styles on security compliance behavior: a preliminary analysis. SIG ICT in Global Development, 10th Annual Pre-ICIS Workshop, Seoul, Korea (2017).

14.Ng, B.-Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: a health belief perspective. Decision Support Systems 46(4), 815-825 (2009).

15.Nosek, B.A., Banaji, M.R., Greenwald, A.G.: Harvesting implicit group attitudes and beliefs from a demonstration web site. Group Dynamics: Theory, Research, and Practice 6(1), 101-115 (2002).

16.Ifinedo, P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. Computers & Security 31(1), 83-95 (2012).

17.Vance, A., Siponen, M., Pahnila, S.: Motivating IS security compliance: insights from habit and protection motivation theory. Information & Management 49(3–4), 190–198 (2012).

18.Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L.: Gender difference and employees' cybersecurity behaviors. Computers in Human Behavior 69, 437-443 (2017).

19.Rowe, A.J., Boulgarides, J.D.: Decision styles—a perspective. Leadership & Organization Development Journal 4(4), 3-9 (1983).

20.Henderson, J.C., Nutt, P.C.: The influence of decision style on decision making behavior. Management Science 26(4), 371-386 (1980).

21.Niu, H.-J.: Cyber peers' influence for adolescent consumer in decision-making styles and online purchasing behavior. Journal of Applied Psychology 43(6), 1228–1237 (2013).

22.International Monetary Fund: Regional economic outlook: Sub-Saharan Africa. World Economic and Financial Surveys, pp. 123 (2015).

23.World Economic Forum, https://www.weforum.org/agenda/2015/08/why-smes-are-key-to-growth-in-africa/, last accessed 2018/07/29.

24.Banker, R.D., Natarajan, R.: Evaluating contextual variables affecting productivity. Operations Research 56(1), 48-58 (2008).

25.Samoilenko, S.: Overview on data envelopment analysis. Advances in research methods for information systems research, pp. 139-150. Springer, Boston, MA (2014).

26.Ayabakan, S., Bardhan, I.R., Zheng, Z.: A data envelopment analysis approach to estimate IT-enabled production capability. MIS Quarterly 41(1), 189-205 (2017).

27.Samoilenko, S., Osei-Bryson, K.M.: Using data envelopment analysis (DEA) for monitoring efficiency-based performance of productivity-driven organizations: design and implementation of a decision support system. Omega 41(1), 131-142 (2013).

28.Banker, R.D., Charnes, A., Cooper, W.W.: Some models for estimating technical and scale inefficiencies in data envelopment analysis. Management Science 30(9), 1078-1092 (1984).

29.Behera, A.K., Verbert, J., Lauwers, B., Duflou, J.R.: Tool path compensation strategies for single point incremental sheet forming using multivariate adaptive regression splines. Computer-Aided Design 45(3), 575-590 (2013).

30.Osei-Bryson, K.M.: A hybrid decision support framework for generating & selecting causal explanatory regression splines models for information systems research. Information Systems Frontiers 17(4), 845-856 (2015).

31.Hastie, T., Tibshirani, R., Friedman, J.: The elements of statistical learning: data mining, inference, and prediction. Springer, New York (2001).

32.Hastie, T., Tibshirani, R.: Generalized additive model. Chapman and Hall, London (1990).

33.Rowe, A.J., Mason, R.O.: Managing with style: a guide to understanding assessing, and improving decision making. Jossey-Bass, San Francisco, CA (1987).